INTERNAL REVENUE SERVICE
IRS Fact Sheet

Media Relations Office | Washington, D.C. | Media Contact: 202.622.4000
www.IRS.gov/newsroom | Public Contact: 800.829.1040

Identity Theft e-Mail Scams a Growing Problem

FS-2008-9, January 2008

The Internal Revenue Service has issued an increasing number of warnings over the last few years about e-mail scams targeting individuals, businesses, exempt organizations and other taxpayers. The scams, popularly known as “phishing” scams, use phony e-mails that falsely claim to come from the IRS.

What Is Phishing?

Phishing — a word play on “fishing” for information — is a scam in which Internet fraudsters send seemingly legitimate e-mail messages to trick unsuspecting victims into revealing personal and financial information, such as a Social Security number (SSN), that can be used to steal the victims’ identity and gain access to the victim’s finances

Alternately, the purpose of an e-mail scam may be to download malware, or malicious code, onto the recipient’s computer when the recipient opens an attachment to the e-mail or clicks on a link within the e-mail. The malware could take over the victim’s computer hard drive, giving someone remote access to the computer, or it could look for passwords and other information and send them to the scamster. There are other types of malware, as well.

The Goal of Identity Theft and Phishing

Typically, identity thieves use someone’s personal data to empty the victim’s financial accounts, run up charges on the victim’s existing credit cards, apply for new loans, credit cards, services or benefits in the victim’s name, file fraudulent tax returns or even commit crimes. Most of these fraudulent activities can be committed electronically from a remote location, including overseas. Committing these activities in cyberspace allows scamsters to act quickly and cover their tracks before the victim becomes aware of the theft.

People whose identities have been stolen can spend months or years — and their hard-earned money — cleaning up the mess thieves have made of their reputations and credit records. In the meantime, victims may lose job opportunities, may be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit.

How the Scams Work

Not all of the scams are conducted through e-mail. Some are conducted by phone or fax. Additionally, identity thieves may go through trash looking for discarded tax returns,

bank records, credit card receipts or other records containing personal and financial information.

Frequently, however, the scams are conducted through the Internet in the form of a phishing scheme. Typically, those that use the IRS as the bait begin with an e-mail that is sent out using the same techniques employed by "spammers." Hundreds of thousands of messages are sent to potential victims advising them that they are under investigation by the IRS or that they have a refund pending from the IRS or they use some other message that sounds legitimate. Some scams attempt to capitalize on current events. To get the victim to respond, a phishing e-mail may threaten a dire consequence or dangle bait, such as a tax refund.

Often, the e-mail or an attachment asks the intended victim to click on a link to access the IRS Web site. The link connects the victim to a Web site that appears authentic and then prompts the victim for personal identifiers, bank or credit card account numbers or PINs.

The phony Web sites appear legitimate because the appearance and much of the content are directly copied from an actual page on the IRS Web site and are then modified by the phishers for their own purposes. The bogus site might look like the IRS.gov home page or may appear to be one of the pages, such as the "Where's My Refund?" page, within the IRS.gov Web site.

Genuine IRS Web site

The only genuine IRS Web site is IRS.gov. All IRS.gov Web page addresses begin with http://www.irs.gov/. Anyone wishing to access the IRS Web site should initiate contact by typing the IRS.gov address into their Internet address window, rather than clicking on a link in an e-mail.

IRS Does Not Ask for Personal Information via e-Mail

As a rule, the IRS does not send unsolicited e-mails to taxpayers, though on occasion some taxpayers might receive newsletters or announcements of upcoming IRS-sponsored events based on their membership in professional tax organizations. However, the IRS does not send unsolicited, tax-account related e-mails to taxpayers.

For security and other reasons, the IRS never asks for personal and financial information via e-mail. Additionally, the IRS never asks people for the PIN numbers, passwords or similar secret access information for their credit card, bank or other financial accounts.

Since the IRS rarely contacts taxpayers via e-mail, and never about their tax accounts, taxpayers should be cautious about any e-mails that claim to come from the IRS.

How to Spot a Scam

Many e-mail scams are fairly sophisticated and hard to detect. However, there are signs to watch for, such as an e-mail that:

- Requests personal and/or financial information, such as name, SSN, or bank or credit card account numbers, either in the e-mail itself or on another site to which a link in the e-mail sends the recipient.
- Dangles bait to get the recipient to respond to the e-mail, such as mentioning a tax refund or offering to pay the recipient to participate in an IRS survey.
- Threatens a consequence for not responding to the e-mail, such as blocking access to the recipient's funds.
- Gets the Internal Revenue Service name wrong.
- Uses incorrect grammar or odd phrasing (many of the e-mail scams originate overseas and are written by non-native English speakers).
- Uses a really long address in any link contained in the e-mail message or one that does not include the actual IRS Web site address. To see the link address, move the mouse over the link included in the text of the e-mail.

Report Scam e-Mails to the IRS

The IRS can use the information, URLs and links in the suspicious e-mails to trace the hosting Web site and alert authorities to help shut down the fraudulent sites.

Taxpayers who receive an unsolicited e-mail communication claiming to be from the IRS can forward the message to phishing@irs.gov using instructions posted on IRS.gov.

To date, the IRS has received almost 33,000 forwarded scam e-mails, reflecting more than a thousand different incidents. Investigations by the Treasury Inspector General for Tax Administration have identified host sites in numerous countries, including Argentina, Aruba, Australia, Austria, Canada, Chile, China, England, Germany, Indonesia, Italy, Japan, Korea, Malaysia, Mexico, Poland, Singapore and Slovakia, as well as the United States.

What Scam Victims Should Do

Any unauthorized activity should be reported to law enforcement authorities and to the three major credit bureaus. More information on how to handle actual or potential identity theft may be found in IRS Publication 4535, Identity Theft Protection and Victim Assistance.

For More Information

Additionally, taxpayers should take steps to protect themselves in advance against potential identity theft.

More information on phishing, identity theft and scams can be found on IRS.gov in various Web articles and news releases. Start with Suspicious e-Mails and Identity Theft and How to Protect Yourself from Suspicious E-Mails or Phishing Schemes.

For more information on understanding and preventing identity theft and suspicious e-mails (phishing), or dealing with their aftermath, check out the following federal resources:

- Department of the Treasury's Identity Theft Resource Page
- Federal Trade Commission's (FTC) Consumer Web Site
- FTC's OnGuardOnLine Web site
- Firstgov
- Social Security Administration (SSA)

—30—